SPOTLIGHT

Sponsored by: Cameyo

Secure, cloud-first operating systems and virtual app delivery are becoming key enablers of enterprises' digital operations and talent strategies.

Accelerating Enterprise Adoption of Cloud-First Operating Systems with Virtual App Delivery

May 2023

Written by: Shannon Kalvar, Research Director, Virtual Client Computing

AT A GLANCE

KEY STAT

IDC research found that in 2022, two years after the pandemic began, 40% of companies were still struggling with providing equal access to enterprise resources for employees engaged in hybrid work.

Introduction

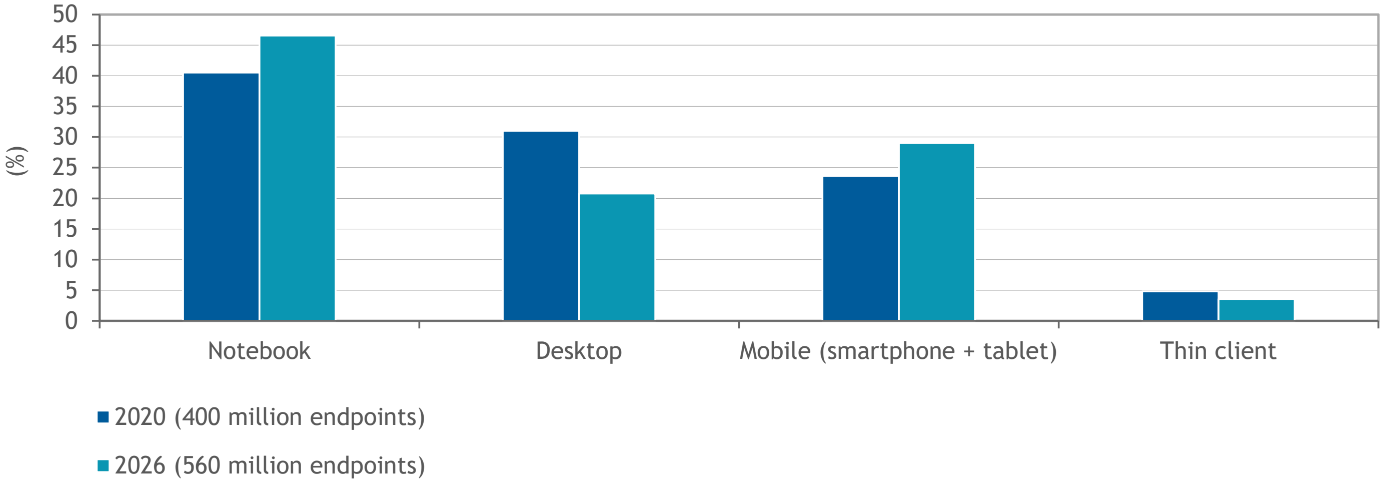
IDC sees the next five years of business as being the evolution from "digital transformation" to "digital operations," the state in which business is conducted and driven and flows through value chains that must be optimized in a hybrid digital-physical world. This transition will have a profound impact on what employees want from their enterprise experience, starting with the endpoint they use and the paths they take to access the enterprise's digital estate.

At the same time, IT departments all over the world struggle to match their ability to provide robust, secure access to a geographically and technologically diverse workforce with diminished resources and potentially diminished budgets. IDC research indicates that over 76% of CIOs expect a recession in the near future (12–24 months), and over a third are worried about the impact of inflation on end-user devices. But changing course will be difficult. In a November 2022 IDC survey, over 81% of IT executives said they experienced digital transformation delays of 1–10 months due to a lack of IT skills (source: *Toward Skilling Excellence: The IDC 2022 Global Skills Survey*).

Toward an Equal Access Future

IDC research found that in 2022, two years after the pandemic began, 40% of companies were still struggling with providing equal access to enterprise resources for employees engaged in hybrid work. Security challenges, diverse network topologies, and a confusing mix of access methods — the usual rogues' gallery of challenges for remote access — topped the list of reasons for the continued struggles with providing equal access. However, underlying these obvious challenges is a profound shift in the devices and form factors used to access corporate applications, data, and services (see Figure 1).

FIGURE 1: ***Mix of Endpoints Accessing Virtualized Apps***



Source: IDC, 2022

There has been a profound shift in the form factors associated with computing, one that will continue as we adapt to hybrid work models. We have moved away from desktops generally, and more specifically from accessing virtualized computing from desktops, to a more flexible model using both laptops and mobile devices — with mobile devices reserved for quick tasks and laptops (including Chromebooks) for more general work. This shift drives a change in operating approaches, power consumption, and support requirements, which in turn creates a need for new features, lighter operating systems, and extended remote management functionality.

Not shown in Figure 1, but equally profound, is an underlying shift in the length of service of laptops (and endpoint devices in general). As enterprises plan for an extended period of economic slowness, they are anticipating extending the life of devices from three years to roughly five years. This will bring with it an array of new challenges, both practical in terms of supporting devices and more subtle in terms of the increased energy consumption of older processors as they struggle to keep up with the operating requirements of more complex operating systems.

Taken together, these shifts (in device mix, computing requirements, usage pattern, and device life span) will create what is, viewed through traditional endpoint management doctrine, a distressingly diverse landscape, prone to security breaches and operational issues. This complexity seems at odds with the need to provide secure, equal access. So, what has changed?

Solving for Diversity

In the past, organizations typically drove down security risk and operational costs by purchasing large numbers of functionally identical devices and then worked to optimize the management of those specific devices. Exceptions were granted only in rare and isolated cases, often provisioned by complex security platforms. In such a setting, either virtual desktop infrastructure (VDI) or virtual application delivery (VAD) would be used to ensure application compatibility with a limited range of endpoints, often when legacy applications could not be affordably brought into the mono-device culture.

Hybrid work — working from many places, at many times, on devices that make sense for both the work task and the physical environment — forces IT departments to radically rethink how they approach the devices they provision to employees. As previously mentioned, immobile desktops give way to mobile devices and semi-portable laptops. The number and type of devices begin to diversify as well, driven by a combination of new use cases, supply limitations, and employee preferences.

The "hybrid" nature of work also extends temporally — individual employees may stay only for a short time, making it logistically or financially challenging to provide everyone with the same kind of device, the same access, and the same tools.

This hybridization of work, devices, and time creates new opportunities for the application of both VDI and VAD. Some of these opportunities are discussed in the remainder of this paper.

Hybrid work — working from many places, at many times, on devices that make sense for both the work task and the physical environment — forces IT departments to radically rethink how they approach the devices they provision to employees.

Solving for Longevity

Economic uncertainty has been the name of the game since the COVID pandemic started in 2020. Shocks from the measures taken to address the pandemic's early days will likely continue until at least 2026. In response, organizations have asked IT to extend the life span of their devices while engaging in the individualized matching required for hybrid work.

Solving for longevity is not going to usher in the "year of the thin client." It will, however, drive organizations to increasingly redeploy older devices with cloud-first operating systems such as ChromeOS as hardware refresh cycles come up. It will also prompt organizations to use these cloud-first operating systems as a way of extending the useful life of existing devices, such as with ChromeOS Flex, which enables organizations to repurpose decommissioned PCs and Macs as ChromeOS devices. These devices will then need some way to access the applications and data the enterprise needs to present to the hybrid workforce, in a secure fashion.

Thriving with Diversity and Longevity While Delivering Equal Access

VAD bridges the gap between the needs of the hybrid workforce and the challenges of the hybrid device ecosystem. It allows the enterprise to apply the speed and security of applications, desktops, or other digital environments directly to any device, with security both on the endpoint and embedded into the delivery mechanism. The enterprise also gains control over the times and places the application can be accessed as well as the ability to monitor user behaviors and respond more closely when there are deviations from expected patterns.

Cloud-first operating systems also seem to have a positive impact. Organizations using ChromeOS, for example, recently reported as much as 44% reduced operating costs over a three-year period, according to an IDC Business Value Study. This savings comes from a combination of security, management, and device-level factors and can include savings from using Chromebook hardware with ChromeOS optimizations.

Benefits

Although both VAD and ChromeOS have independent strengths, the two bring greater benefits when fully integrated with one another, particularly considering the extensive technical integrations undertaken by Cameyo and Google over the past few years. These benefits include but are not limited to:

- **Isolated security surface.** Zero trust is a design, but practically any access point is a threat surface. With VAD and ChromeOS, IT can deliver all the apps and data that users need to be productive without that device being connected to the corporate network. This separates the device from the enterprise network and separates the apps from the device, allowing more opportunities for hardening and threat isolation.
- **Lower operating cost.** Operations account for roughly 70% of the total cost of a system over time. The more complex the system, and the more skilled administrators are needed to manage it, the greater this burden becomes. Logically, we would expect that the combination of a low-weight OS and VAD would lead to greater simplicity and lower cost. In fact, IDC research indicates that virtualization by itself reduces the total cost per employee per seat over time by 6% for enterprises and 9% for small and medium-sized businesses.
- **Simplified problem solving.** As organizations move into digital operations, they cannot wait days to resolve problems or deploy solutions. The isolation of applications from endpoints and endpoints from the enterprise allows for rapid identification and resolution of common problems, with many instances of application performance problem resolution being fully automated from detection to resolution and manual identification of problems in application performance taking on average 1.8 days.
- **Enhanced user experience.** While increased security, reduced costs, and improved performance are all critical, none can happen at the expense of an organization's overall productivity. IT needs to provide users with seamless access to all the apps they need to be productive, without introducing any friction that interrupts users' workflows. With Cameyo's VAD and ChromeOS, users can access and utilize all their apps as if the apps were installed locally, with nothing new to learn.

Key Trends

IDC research shows both a demographic shortage and a skills shortage in IT operations: Organizations cannot find people with the right skills, and there are simply not enough people to do the work as it is currently organized. This leads to a dramatic rise in the need for automated observation and resolution of problems as well as a marked increase in the need for automation skills. These needs form an unfortunately vicious cycle: Enterprises need automation to overcome their challenges, but the IT resources they need to do so are the very ones they cannot find.

This shortage is especially acute when looking at niche skills such as those needed to run traditional VDI platforms. These platforms, while exceptionally powerful, require specialized training to architect, install, and operate over an extended period. The pandemic era created higher demand for these skills at precisely the time IT staff were also under personal stress, leading to a rapid decline in the number of VDI experts available for projects. This shortage has already delayed projects by as much as 10 months and is not projected to improve.

The challenges in IT are just part of a broader trend in the largest economies, where aging populations, slow immigration, and lower birth rates combined with high educational attainment have created a dynamic in which it is hard to hire, engage, and retain employees with sought-after skills. To resolve these challenging demographic and skills issues, employers will increasingly draw from talent pools outside of their immediate geographic area. This will increase the need for adaptability around the endpoint, forcing employers to make decisions about how to best align their physical/digital experience with their employee engagement and retention strategy.

Considering Cameyo and ChromeOS

So, how do organizations reconcile the seemingly competing demands of enabling equal access for all users, on secure devices, and addressing cost issues and the need for longevity — all in a resource-constrained IT environment?

This confluence of requirements is part of what has led to the accelerated adoption of VAD solutions such as Cameyo, especially in conjunction with a secure and cost-effective device strategy enabled by ChromeOS.

Cameyo is one of the pioneers in cloud-based VAD, which provides an ultra-secure, simple, and cost-effective way to deliver all apps — legacy Windows, Linux, internal web, and SaaS — to any device without the need for legacy virtual desktops or VPNs. Unlike traditional VDI and DaaS solutions, Cameyo is a cloud-native virtualization solution that delivers any application to any device without delivering the Windows OS.

Google's ChromeOS has long been known for security, cost-effectiveness, and manageability; in recent years, the adoption of ChromeOS in the enterprise has accelerated. IDC research reveals that ChromeOS provides enterprise users with a 245% ROI over three years while also being 63% faster to deploy, enabling a 37% reduction in device costs, and delivering 77% higher productivity.

Key differentiators of Cameyo's approach to VAD include:

- **Simplicity.** Organizations can get started with Cameyo and have their apps delivered to users in hours, not weeks or months — all without requiring the specialized expertise needed to deploy and maintain virtual desktop systems.
- **Zero trust security.** Cameyo is designed with a zero trust security model that eliminates the need for VPNs or open firewall or server ports.
- **Cost-effectiveness.** Cameyo reportedly saves organizations, on average, up to 70% over legacy VDI and desktop-as-a-service (DaaS) products. Cameyo has simple per-user, per-month pricing that includes all usage fees and remote desktop server (RDS) client access licenses (CALs) (in the fully hosted version).
- **Flexibility.** Cameyo's cloud-native service works in any cloud, hybrid, or on-premises environment and integrates with an organization's existing single sign-on (SSO), databases, and more.
- **Seamless user experience.** Cameyo's ability to deliver any app as a progressive web application (PWA) plus the company's deep integration with ChromeOS enables end users to simply click and use their applications as if they were installed locally, with nothing new to learn.

While the Cameyo platform enables organizations to deliver any app to any device, its integration with ChromeOS is a significant focus and delivers a native application experience for enterprise end users on ChromeOS devices.

Google has certified Cameyo as a Chrome Enterprise Recommended solution for virtualization, and Cameyo helps overcome the legacy application barrier that often causes organizations to hesitate when it comes to fully adopting ChromeOS throughout the enterprise.

Challenges

Knowledge work, particularly work that involves a wide range of human and digital collaborations, requires a robust ecosystem of not just endpoints but also peripheral devices. Application virtualization approaches, including those based in the cloud, tend to rely on the endpoint and endpoint operating system to manage this issue. Unfortunately, decades of virtualization experience, as well as field reports, suggest that this "offloaded" approach to the device ecosystem will not work in many practical cases. In fact, it may drive up support and operational costs in the short to medium term as the organization discovers previously working parts of its hybrid workspace no longer function in a virtualized delivery approach.

Adaptive technology must extend to include learning and sensory styles, adapting the applications themselves to very different ways of working, for this hybrid work future to succeed at scale. Doing so requires more than just projecting and virtualizing applications; it requires rethinking the interface and how users interact with that interface. In fact, nearly 60% of organizations see adapting to nonvisual operations as a key element in their overall intelligent digital workspace experience (source: *Adaptive Technology in the Virtual Client and Digital Workspace*, IDC Survey Spotlight, February 2023). This will mean a break in the uniform approach provided by virtualization — the interface may need to adapt to tactile, audio, and other modes beyond the visual "lock-in" common in today's applications.

Virtualization is also, by necessity, sensitive to a wide range of factors outside of enterprise control, including power concerns across the delivery grid, network disruptions in third-party providers, and issues with the clouds used to deliver the goods and services. Local applications and robust endpoints, for all their faults, work even in otherwise adverse conditions. A mix will always be necessary — a mix that must be carefully matched to talent and technical strategy in this hybrid work world.

Conclusion

Organizations shifting into digital operations no longer have the luxury of having homogeneous fleets of devices, abundant technical talent, and comparatively simple operating environments. Instead, they must meet the demands of hybrid environments — hybrid cloud, hybrid devices, hybrid workforces, hybrid workstyles — where and when they occur with the staff they have on hand. Meeting these demands, though, cannot compromise the organization's security posture or productivity.

Secure, cloud-first operating systems and VAD thus become key enablers of the enterprise's digital operations and talent strategies. Combining Cameyo's VAD solution with ChromeOS devices enables enterprises to continue to pursue strategic imperatives while increasing security, lowering costs, improving the user experience for greater productivity, and extending the life span of devices. This results in a win-win scenario for both end users and IT. End users get seamless and productive work experiences from anywhere, and IT gets a more secure, flexible, and cost-effective solution that requires fewer IT resources to deploy and manage.

About the Analyst

Shannon Kalvar, *Research Director, Virtual Client Computing*

Shannon Kalvar is Research Manager for IDC's IT Service Management and Client Virtualization Program, responsible for delivering research and advisory for IT executives, vendor management teams, and investment executives. Mr. Kalvar's research coverage includes IT service management, desktop as a service (DaaS), virtual client computing, cost transparency tools, software asset management, and the use of AI and NLP for service management.

MESSAGE FROM THE SPONSOR

More About Cameyo & ChromeOS

Cameyo's Virtual App Delivery (VAD) platform provides a secure, simple, and cost-effective cloud desktop solution for delivering all your apps – legacy Windows, internal web, and SaaS – to ChromeOS devices as PWAs without the need for legacy Virtual Desktops or VPNs. Cameyo integrates deeply with ChromeOS and Google Admin console, providing end users with a native app experience while enabling IT teams to publish and push apps directly to their users' taskbars on ChromeOS. Together, ChromeOS and Cameyo provide end users with seamless productivity while enabling your organization to reduce complexity, enhance security, and lower costs.

To test out the power of ChromeOS and Cameyo, check out the bundle offer here.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.